

LISTING OF THE CLAIMS

CLAIMS

What is claimed, is:

1. (Currently amended) A method comprising of monitoring network activities as a time-ordered sequence of events in a computer network, each event having attributes triggered by an intrusion-detection system, each event being characterized by a given set of attributes called dimensions, each event forming an n-dimensional space, the step of monitoring method comprising:

said computer network triggering said events, each event being provided with attribute values allocated to a given set of attributes of said each event, each attribute having a particular attribute value,

simultaneously monitoring each particular attribute value of various event attributes from said given set of attributes versus the arrival time of said each event,

providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting a time period and the y-axis presenting an attribute value range, and visualizing data along said x and y coordinate axes, said axes being attribute axes,

determining a primary attribute of said each event, said primary attribute being selected from the given set of attributes, each said primary attribute of said each event to be presented with its a corresponding attribute values value on the y-axis of the cross plot,

allocating a first display label to the events indicating the attribute ~~values~~ value of the primary attribute of each event, providing a pattern algorithm to detect whether an arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to the given pattern and

1 of the attributes assigned to the arrived event, providing a mapping algorithm to map any attribute
2 value of an attribute selected from the given set of attributes onto the y-axis of the cross plot,
3 allocating a second display label to said each event indicating the attribute values of the attributes
4 being uncovered as part of the given pattern,
5 plotting all events that arrived within the time period and including an attribute value allocated to
6 the primary attribute into the cross plot with the first display label indicating the primary attribute,
7 the position of the first display label of said each event in the cross plot being determined on the
8 basis of the attribute value of the primary attribute of the event and its arrival time,
9 plotting all events that arrived within the time period and being detected by means of the pattern
10 algorithm as part of the given pattern into the cross plot with the second display label indicating
11 the given pattern, the position of the second display label of said each event in the cross plot
12 being determined by the mapping algorithm on the basis of the attribute value of the attribute of
13 the event being uncovered as part of the given pattern and its arrival time,
14 viewing a secondary attribute of said each event together with the primary attribute on said
15 display; and
16 ~~automatically generating a large variety of visualizations along other attribute axes, and~~
17 ~~identifying correlations by superimposing and cross-referencing these visualizations.~~

18 2. (original) The method according to claim 1, further comprising:

19 recording the attribute values and the arrival time of a new event, determining on the basis of the
20 recorded attribute values of event whether or not the newly arrived event includes an attribute
21 value of the primary attribute, and if the newly arrived event includes the attribute value for the
22 primary attribute shifting the x-axis of the cross plot so that the time period being presented on
23 the x-axis covers the arrival time of the event, and

1 plotting the event arrived within the shifted time period into the cross plot with the first display
2 label indicating the primary attribute.

3 3. (original) The method according to claim 2 comprising the further steps of:

4 determining on the basis of the recorded attribute values of event whether or not the newly
5 arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to
6 the given pattern and of the attributes assigned to the arrived event,

7

8 if the newly arrived event includes an attribute value of the given pattern adding the event to the
9 previous events being detected as part of the given pattern, and

10 redrawing all the events being associated with given pattern in the cross plot.

11 4. (previously presented) The method according to claim 3, further comprising:

12 if the newly arrived event does not include an attribute value of the given pattern, determining on
13 the basis of the recorded attribute values of all previous arrived events by means of the pattern
14 algorithm whether or not the newly arrived event is part of a new pattern on the basis of a
15 comparison of the attributes allocated to the new pattern and of the attributes assigned to the
16 arrived events;

17 if the newly arrived event forms together with previous recorded events the new pattern,
18 allocating a third display label to the events indicating the attribute values of the attributes being
19 uncovered as part of the new pattern; and

20 plotting the all events being detected by means of the pattern algorithm as part of the new pattern
21 into the cross plot with the third display label indicating the new pattern, the position of the third
22 display label of said each event in the cross plot being determined by the mapping algorithm on

1 the basis of the attribute value of the attribute of the event being uncovered as part of the new
2 pattern and its arrival time.

3 5. (previously presented) The method according to claim 1 , further comprising:

4 removing all the events including an attribute value allocated to the primary attribute from the
5 cross plot, if a primary attribute to be presented with its attribute values on the y-axis of the cross
6 plot is changed, allocating a fourth display label to the events indicating the attribute values of the
7 new primary attribute, and

8 plotting all the events arrived within the time period and including an attribute value allocated to
9 the new primary attribute into the cross plot with the fourth display label indicating the new
10 primary attribute, the position of the fourth display label of said each event in the cross plot being
11 determined on the basis of the attribute value of the primary attribute of the event and its arrival
12 time.

13 6. (original) The method according to claim 1 comprising the further steps of plotting all
14 attribute values recorded for an event with the respective display label into the cross plot if the
15 event is selected by an operator, and displaying textual information associated with the selected
16 event on the event display.

17 7. (original) The method according to claim 1, wherein the pattern algorithm is suitable to
18 perform multi-attribute pattern recognition.

19 8. (original) The method according to claim 1, wherein each display label includes a specific color
20 and/or a specific mark layout.

21 9. (original) The method according to claim 1, wherein all events being uncovered as part of the
22 pattern are clustered by the corresponding display label.

1 10. (Currently amended) A method according to claim 1, further comprising employing a
2 computer readable program on tangible computer ~~media~~ readable medium and being
3 computer executable instructions, comprising program code to cause the carrying out the
4 steps of triggering, monitoring, providing, determining, allocating a first display label,
5 allocating a second display label, plotting events including an attribute value, plotting
6 events detected, viewing, and automatically generating, when the program code is running
7 on a computer.

8 11. (Currently amended) A computer program *on a computer readable medium* ~~containing a~~
9 comprising program code being computer executable instructions to carry out all steps of
10 the method of claim 1, said program code being stored on data carrier.

11 12. (previously presented) An event visualization device for monitoring events in a computer
12 network, the device comprising means to perform all steps of the method as claimed in
13 claim 1.

14 13. (previously presented) An article of manufacture comprising a computer readable medium
15 having computer readable program code means embodied therein for causing monitoring of
16 events in a computer network, the computer readable program code means in said article of
17 manufacture comprising computer readable program code means for causing a computer to effect
18 all steps of claim 1.

19 14. (Currently amended) A program storage device being a computer readable medium, tangibly
20 embodying a program of instructions executable by ~~the machine~~ a computer to perform method
21 steps for monitoring network activities as a time-ordered sequence of events in a computer
22 network, each event having attributes triggered by an intrusion-detection system, each event
23 being characterized by a given set of attributes called dimensions, each event forming an
24 n-dimensional space, said step of monitoring ~~method steps~~ comprising the steps of:

1 said computer network triggering said events, each event being provided with attribute values
2 allocated to a given set of attributes of said each event, each attribute having a particular attribute
3 value,

4 simultaneously monitoring each particular attribute value of various event attributes from said
5 given set of attributes versus the arrival time of said each event,

6 providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting
7 a time period and the y-axis presenting an attribute value range, and visualizing data along said x
8 and y coordinate axes, said axes being attribute axes,

9 determining a primary attribute of said each event selected from the given set of attributes, each
10 said primary attribute of said each event to be presented with ~~its~~ a corresponding attribute ~~values~~
11 value on the y-axis of the cross plot,

12

13 allocating a first display label to the events indicating the attribute ~~values~~ value of the primary
14 attribute of each event providing a pattern algorithm to detect whether an arrived event is part of
15 the given pattern on the basis of a comparison of the attributes allocated to the given pattern and
16 of the attributes assigned to the arrived event, providing a mapping algorithm to map any attribute
17 value of an attribute selected from the given set of attributes onto the y-axis of the cross plot,

18 allocating a second display label to said each event indicating the attribute values of the attributes
19 being uncovered as part of the given pattern,

20 plotting all events that arrived within the time period and including an attribute value allocated to
21 the primary attribute into the cross plot with the first display label indicating the primary attribute,
22 the position of the first display label of said each event in the cross plot being determined on the
23 basis of the attribute value of the primary attribute of the event and its arrival time,

plotting all events that arrived within the time period and being detected by means of the pattern algorithm as part of the given pattern into the cross plot with the second display label indicating the given pattern, the position of the second display label of said each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event being uncovered as part of the given pattern and its arrival time, and

viewing a secondary attribute of said each event together with the primary attribute on said display; ~~and~~

~~automatically generating a large variety of visualizations along other attribute axes, and identifying correlations by superimposing and cross-referencing these visualizations.~~

15. (previously presented) A computer program product comprising a computer readable medium having computer readable program code means embodied therein for causing the event visualization device, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect all functions of claim 12.

16. (previously presented) The method according to claim 1, further comprising:

recording the attribute values and the arrival time of a new event, determining on the basis of the recorded attribute values of event whether or not the newly arrived event includes an attribute value of the primary attribute, and if the newly arrived event includes the attribute value for the primary attribute shifting the x-axis of the cross plot so that the time period being presented on the x-axis covers the arrival time of the event,

plotting the event arrived within the shifted time period into the cross plot with the first display label indicating the primary attribute;

- 1 determining on the basis of the recorded attribute values of event whether or not the newly
- 2 arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to
- 3 the given pattern and of the attributes assigned to the arrived event;
- 4 if the newly arrived event includes an attribute value of the given pattern adding the event to the
- 5 previous events being detected as part of the given pattern;
- 6 redrawing all the events being associated with given pattern in the cross plot;
- 7 if the newly arrived event does not include an attribute value of the given pattern, determining on
- 8 the basis of the recorded attribute values of all previous arrived events by means of the pattern
- 9 algorithm whether or not the newly arrived event is part of a new pattern on the basis of a
- 10 comparison of the attributes allocated to the new pattern and of the attributes assigned to the
- 11 arrived events;
- 12 if the newly arrived event forms together with previous recorded events the new pattern,
- 13 allocating a third display label to the events indicating the attribute values of the attributes being
- 14 uncovered as part of the new pattern; and
- 15 plotting the all events being detected by means of the pattern algorithm as part of the new pattern
- 16 into the cross plot with the third display label indicating the new pattern, the position of the third
- 17 display label of each event in the cross plot being determined by the mapping algorithm on the
- 18 basis of the attribute value of the attribute of the event being uncovered as part of the new pattern
- 19 and its arrival time;
- 20 17. (previously presented) The method according to claim 16, further comprising:
- 21 removing all the events including an attribute value allocated to the primary attribute from the
- 22 cross plot, if a primary attribute to be presented with its attribute values on the y-axis of the cross

1 plot is changed, allocating a fourth display label to the events indicating the attribute values of the
2 new primary attribute, and

3 plotting all the events arrived within the time period and including an attribute value allocated to
4 the new primary attribute into the cross plot with the fourth display label indicating the new
5 primary attribute, the position of the fourth display label of each event in the cross plot being
6 determined on the basis of the attribute value of the primary attribute of the event and its arrival
7 time.

8 18. (previously presented) The event visualization device for monitoring events in a computer
9 network, according to claim 12, further comprising:

10 means for recording the attribute values and the arrival time of a new event, means for
11 determining on the basis of the recorded attribute values of event whether or not the newly
12 arrived event includes an attribute value of the primary attribute, and if the newly arrived event
13 includes the attribute value for the primary attribute shifting the x-axis of the cross plot so that the
14 time period being presented on the x-axis covers the arrival time of the event,

15 means for plotting the event arrived within the shifted time period into the cross plot with the first
16 display label indicating the primary attribute;

17 means for determining on the basis of the recorded attribute values of event whether or not the
18 newly arrived event is part of the given pattern on the basis of a comparison of the attributes
19 allocated to the given pattern and of the attributes assigned to the arrived event;

20 means for adding for if the newly arrived event includes an attribute value of the given pattern
21 adding the event to the previous events being detected as part of the given pattern;

22 means for redrawing all the events being associated with given pattern in the cross plot;

1 means for determining if the newly arrived event does not include an attribute value of the given
2 pattern, means for determining on the basis of the recorded attribute values of all previous arrived
3 events by means of the pattern algorithm whether or not the newly arrived event is part of a new
4 pattern on the basis of a comparison of the attributes allocated to the new pattern and of the
5 attributes assigned to the arrived events;

6 means for allocating if the newly arrived event forms together with previous recorded events the
7 new pattern, allocating a third display label to the events indicating the attribute values of the
8 attributes being uncovered as part of the new pattern; and

9 means for plotting the all events being detected by means of the pattern algorithm as part of the
10 new pattern into the cross plot with the third display label indicating the new pattern, the position
11 of the third display label of each event in the cross plot being determined by the mapping
12 algorithm on the basis of the attribute value of the attribute of the event being uncovered as part
13 of the new pattern and its arrival time;

14 19. (previously presented) The event visualization device for monitoring events in a computer
15 network, according to claim 18, further comprising:

16 means for removing all the events including an attribute value allocated to the primary attribute
17 from the cross plot, if a primary attribute to be presented with its attribute values on the y-axis of
18 the cross plot is changed, allocating a fourth display label to the events indicating the attribute
19 values of the new primary attribute, and

20 means for plotting all the events arrived within the time period and including an attribute value
21 allocated to the new primary attribute into the cross plot with the fourth display label indicating
22 the new primary attribute, the position of the fourth display label of each event in the cross plot
23 being determined on the basis of the attribute value of the primary attribute of the event and its
24 arrival time.

20. (currently amended) An article of manufacture comprising apparatus for monitoring events in a computer network, the apparatus comprising:

said computer network having means for intrusion-detection triggering said events, each event having attributes triggered by the means for intrusion-detection, each event being characterized by a given set of attributes called dimensions, each event forming an n-dimensional space, each event being provided with attribute values allocated to a given set of attributes of said each event,

means for simultaneously monitoring various event attributes from said given set of attributes versus the arrival time of said each event,

means for providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting a time period and the y-axis presenting an attribute value range, and visualizing data along said x and y coordinate axes, said axes being attribute axes,

means for determining a primary attribute of said each event, said primary attribute being selected from the given set of attributes, each said primary attribute of said each event to be presented with its a corresponding attribute values value on the y-axis of the cross plot,

means for allocating a first display label to the events indicating the attribute ~~values~~ value of the primary attribute of each event, providing a pattern algorithm to detect whether an arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event, providing a mapping algorithm to map any attribute value of an attribute selected from the given set of attributes onto the y-axis of the cross plot,

means for allocating a second display label to said each event indicating the attribute values of the attributes being uncovered as part of the given pattern,

- 1 means for plotting all events that arrived within the time period and including an attribute value
2 allocated to the primary attribute into the cross plot with the first display label indicating the
3 primary attribute, the position of the first display label of said each event in the cross plot being
4 determined on the basis of the attribute value of the primary attribute of the event and its arrival
5 time,
- 6 means for plotting all events that arrived within the time period and being detected by means of
7 the pattern algorithm as part of the given pattern into the cross plot with the second display label
8 indicating the given pattern, the position of the second display label of said each event in the
9 cross plot being determined by the mapping algorithm on the basis of the attribute value of the
10 attribute of the event being uncovered as part of the given pattern and its arrival time, and
- 11 means for viewing a secondary attribute of said each event together with the primary attribute on
12 said display;~~and~~
- 13 ~~means for automatically generating a large variety of visualizations along other attribute axes, and~~
14 ~~identifying correlations by superimposing and cross-referencing these visualizations.~~